

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON

JASON MEYER, an individual;
ARGIL DX LLC f/k/a ZAP
TECHNOLOGY SOLUTIONS LLC, a
Nevada limited liability company; and
ARGIL DX, putative partnership,

Plaintiffs,

v.

ANKUR MITTAL, an individual; AXENO
CONSULTING PVT. LTD. f/k/a
ARGILDX CONSULTING PVT. LTD.
f/k/a ACCUNITY SOFTWARE PVT.
LTD., an Indian private company; and
ADX CONSULTING INC., a Texas
corporation,

Defendants.

No. 3:21-cv-00621-HZ

OPINION & ORDER

Heather Harriman
Eric Lang
Rose Law Firm, P.C.
5200 SW Meadows Rd, Ste 150
Lake Oswego, OR 97035

Attorneys for Plaintiffs

Sara Cotton
Nika Aldrich
Mario Delegato
Schwabe, Williamson & Wyatt, P.C.
1211 SW 5th Ave, Ste 1900
Portland, OR 97204

Attorneys for Defendants

HERNÁNDEZ, District Judge:

Before the Court is Defendants’ Motion for Partial Summary Judgment and for Sanctions. ECF 106. Defendants move for summary judgment on their Stored Communications Act (“SCA”) counterclaim against Plaintiffs Jason Meyer and Argil DX LLC (“Zap”). They also move for sanctions including dismissal of all of Plaintiffs’ causes of action with prejudice, exclusion of certain documents and all evidence derived from those documents, an order that Plaintiffs destroy certain documents and certify to the Court that they have done so, and attorney fees and costs. Finally, Defendants move for limited discovery of Plaintiffs’ counsel’s law firm. For the following reasons, the Court denies the motion.

BACKGROUND

This case arises from a business collaboration that went sour. Plaintiff Jason Meyer is the sole member of Plaintiff Argil DX LLC, formerly known as Zap,¹ a web-design company. Meyer Decl. Opp. Summ. J. ¶ 4, ECF 133. Plaintiffs Meyer and Zap are based in Oregon. *Id.* ¶ 3. Defendant Axeno Consulting was co-founded under the name “Accunity” by Defendant Ankur Mittal in 2014 and is based in India. Mittal Decl. Summ. J. ¶ 4, ECF 107. Axeno and four of its executives, including Defendant Mittal, formed ADX Consulting, a Texas corporation, in September 2020. *Id.* ¶ 20. The goal was to expand Axeno’s presence in the United States. *Id.* The

¹ Due to the similarity of names between Plaintiff entities, the Court will refer to Plaintiff Argil DX LLC as “Zap” and Plaintiff Argil DX, putative partnership, as “the partnership.”

plaintiff partnership is an entity whose existence the parties dispute. Plaintiffs Meyer and Zap assert that Zap and Axeno (then known as Accunity) formed a partnership in 2017. Pl. Resp. 3-4, ECF 134.² Defendants assert that the parties created a joint brand but no partnership. Def. Mot. Summ. J. 5-6. This collaboration was called Argil DX. Meyer Decl. Opp. Summ. J. ¶ 11.

I. The Parties' Collaboration

Plaintiff Meyer and Defendant Mittal held a meeting in Portland, Oregon, in or about February 2017 to discuss their collaboration. *Id.* ¶ 10, Ex. O (accepted calendar invite from Plaintiff Meyer to Defendant Mittal with subject line “Talk about work Plan and Merger”). In March 2017, Defendant Mittal wrote to Plaintiff Meyer, “I think it’s just a beginning of a new journey of our partnership so looking forward to this journey.” *Id.* ¶ 10, Ex. P. In July 2017, the parties created a website for the partnership, Argil DX, with the headline “ZAP Technology Solutions Merges with Accunity Software to form ARGIL DX.” *Id.* ¶ 11, Ex. Q at 1. Defendant Mittal posted about the merger on Twitter. *Id.* at 2.

Following the announcement of merger, Defendant Mittal and Plaintiff Meyer were referred to as co-founders of the partnership. Meyer Decl. Opp. Summ. J. ¶¶ 12-13, Exs. R (organizational chart listing Plaintiff Meyer as CEO/President and Defendant Mittal as President), S (Twitter profile of Defendant Mittal listing him as “MD and Founder, Argil DX”), W (LinkedIn page showing Defendant Mittal as “President at Argil DX” and Defendant Meyer as “CEO of Argil DX”), T (website for Argil DX listing Plaintiff Meyer as “CEO & President Global” and Defendant Mittal as “President, APAC”), U (Facebook page for Argil DX listing location in Beaverton, OR).

² All citations to Plaintiffs’ response to Defendants’ motion for summary judgment refer to Plaintiffs’ Corrected Response.

According to Plaintiff Meyer, the parties devised a system to share revenues from projects. Meyer Decl. Opp. Summ. J. ¶ 14. Plaintiff Meyer states that “[s]hared profits would be calculated on a project-by project basis by deducting a project’s expenses (not including operating and overhead costs) from its revenues.” *Id.* He states that “[t]he difference between Project Revenues and expenses would then be shared between the partners.” *Id.* See also Mittal Decl. Summ. J. Ex. 3 (email from Plaintiff Meyer to Defendant Mittal discussing profit sharing).

Plaintiff Meyer and Defendant Mittal did not sign a document memorializing the merger. Aldred Reply Decl. Ex. 33, Meyer Dep. I 48:9-18, ECF 142. They did not create a written partnership agreement. *Id.* at 57:11-19. According to Plaintiff Meyer, he and Defendant Mittal agreed that they would each be called a co-founder. *Id.* at 58:5-7. Plaintiff Meyer did not recall discussing additional rights or obligations for their respective businesses. *Id.* at 58:17-25. Plaintiff Meyer and Defendant Mittal did not discuss governing law or taxation for the partnership. *Id.* at 60:17-61:7. The parties generally agreed that the respective businesses would handle personnel matters for their own employees. *Id.* at 63:8-64:6.

Defendant Mittal asserts that he never intended to form a partnership and instead expected that Axeno would be a subcontractor for Zap. Mittal Decl. Summ. J. ¶¶ 6, 10. According to Defendant Mittal, “Axeno performed labor and invoiced Zap for those services. Zap invoiced the customers, received the funds, and paid Axeno based on its invoices.” *Id.* ¶ 10. Defendant Axeno continued to pursue projects without Zap, and Plaintiff Zap continued to pursue projects without Axeno. *Id.* ¶ 9, Ex. 1 at 1-2 (messages between Plaintiff Meyer and Defendant Mittal discussing subcontracting opportunities).

II. The Parties' Email Domain and Server

As part of their collaboration, the parties used email addresses with the @argildx.com domain name. Meyer Decl. Opp. Summ. J. ¶ 8. Defendant Mittal acquired the domain name “[i]n support of this joint branding effort.” Mittal Decl. Summ. J. ¶ 8. The parties’ email was provided through a Microsoft Office 365 account. Meyer Decl. Opp. Summ. J. ¶ 8. Zap entered into a subscription agreement with Microsoft for the account in August 2015. *Id.* ¶¶ 5-6. Plaintiff Meyer executed the agreement on behalf of Zap in his capacity as president of Zap. *Id.* ¶ 7. The Office 365 account stored emails sent from and received by the @argildx email addresses in Microsoft’s cloud server. *Id.* ¶ 8. This server space was part of the account to which Zap subscribed. *Id.*

Zap has always paid the monthly subscription fee to Microsoft. *Id.* ¶ 8. Between May 2017 and around December 2021, this fee was divided between Zap and Axeno. *Id.* Plaintiff Meyer was the first global administrator of the Office 365 account and has always been a global administrator of the account. *Id.* ¶ 9. Plaintiff Meyer gave Defendant Mittal global administrator privileges as part of the parties’ collaboration. Mittal Decl. Summ. J. ¶ 15; Meyer Decl. Status Quo ¶ 9, ECF 95; Meyer Decl. Opp. Summ. J. Ex. V (showing that Zap was the organization with the Office 365 subscription). Plaintiff Meyer revoked Defendant Mittal’s administrator access in December 2021. Meyer Decl. Status Quo ¶ 21.

Defendant Mittal moved all of the emails for the business then known as Accunity from a Gmail server to the Microsoft 365 server in or about June 2017. Mittal Reply Decl. ¶ 3, ECF 141. He told Plaintiff Meyer, “I am not comfortable sharing my accunity mail password with” Long Phan, one of Zap’s employees. *Id.* Ex. 32. Plaintiff Meyer responded, “Ok. I understand, but he will (does) have access to the [argildx domain] email. He’s going to be administering it.”

Id. Defendant Mittal then responded, “You mean, he can login as me?” *Id.* Plaintiff Meyer responded, “I don’t think so. But I’m not sure. He has global administrator access. I’m not sure what that means. I would think it would not mean that he can read other people’s email. But that’s a good thing for me to check.” *Id.* Defendant Mittal responded, “I think office 365 allows impersonation. And if that is there, it is not right. Legally as well. We should definitely check that.” *Id.* Plaintiff Meyer then responded that he looked into the issue and “I cannot impersonate anyone unless I go into administration and set it up for each user that I want to be able to impersonate.” *Id.* He offered to have Long Phan sign something related to access. *Id.* Defendant Mittal responded that “I think you should let him know that for any reason if it comes to a point that he needs to access your or mine [sic] account, he should first take an approval.” *Id.* Plaintiff Meyer responded, “Yes, I’ll let him know that if he needs to access anyone’s email account, he needs permission.” *Id.*

A Microsoft 365 account comes with a set of administrative roles that can be assigned to users. Williams Decl. Opp. Summ. J. Ex. H at 1, ECF 131. According to Microsoft’s description, a global administrator has “almost unlimited access to [the] organization’s settings and most of its data.” *Id.* at 2. The person who signs up for the service automatically becomes a global administrator. *Id.* at 4.

Subscribers to a Microsoft 365 account are subject to an online subscription agreement. Williams Decl. Opp. Summ. J. Ex. G. The agreement is between Microsoft and the entity the individual represents or, if there is no designated entity, the individual user. *Id.* at 1. It provides that the subscriber “control[s] access by End Users[.]” *Id.* at 2. “End Users” are defined as “any person [the subscriber] permit[s] to access Customer Data hosted in the Online Services or otherwise use the Online Services, or any user of a Customer Solution.” *Id.* at 10. Per the

subscription agreement, the organization providing a domain name “may assume control over and manage [the subscriber’s] use of the Online Services.” *Id.* at 3. The agreement also provides that the “organization’s designated administrator . . . may (i) control and administer [the subscriber’s] account, including modifying and terminating [the subscriber’s] access and (ii) access and process [the subscriber’s] data, including the contents of [the subscriber’s] communications and files.” *Id.*

Microsoft maintains a publicly available services agreement on its website. Williams Decl. Opp. Summ. J. Ex. C (agreement as it appeared on Microsoft’s website on January 25, 2021). The agreement states that a user accepts the terms of service by creating a Microsoft account, using the services, or continuing to use the services after being notified of a change to the terms of service. *Id.* at 3. The terms of service reference and link to Microsoft’s privacy statement. *Id.* The terms of service also advise: “If you received your Microsoft account from a third party, the third party may have additional rights over your account, like the ability to access or delete your Microsoft account.” *Id.* at 5. The terms of service further provide that if a user signs in with a work or school email address, the user (referred to as “you”) “agree that the owner of the domain associated with your email address” may “control and administer your account, and access and process your Data, including the contents of your communications and files[.]” *Id.* at 6. The terms of service as updated in June 2022 also contain these terms. Williams Decl. Opp. Summ. J. Ex. D at 4, 6, 7.

Microsoft’s privacy statement, as updated in December 2022, contains the following language:

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account, that organization can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.

- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of a change of employment, for example), you may lose access to the products and content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Williams Decl. Opp. Summ. J. Ex. E at 15. The change history reflects that this portion of the privacy statement has been edited in the time since Defendant Mittal was given access to Plaintiff Meyer's account. Williams Decl. Opp. Summ. J. Ex. F at 8 (changes in October 2018), 10 (changes in May 2018).

Plaintiff Meyer and other global administrators, including Defendant Mittal, received emails from Microsoft when certain actions associated with the Office 365 account occurred. Meyer Decl. Opp. Summ. J. ¶ 18, Ex. V. The footers of these emails contained a hyperlink to Microsoft's privacy policy. *Id.*

III. The Parties' Relationship Sours

Unfortunately, the parties' business relationship grew strained due to financial concerns. In August 2019, Defendant Mittal emailed Plaintiff Meyer to advise that the India office did not have enough funds to cover office expenses for the next month. Mittal Decl. Summ. J. Ex. 5 at 3-4. He told Plaintiff Meyer that they needed to "discuss this and find a way out." *Id.* at 4. Plaintiff Meyer responded the next day, saying, "I know that things have not gone the way that either of us expected when we started this company." *Id.* at 1. He acknowledged "significant debt from the U.S. company to the India company." *Id.* at 2. He proposed strategies for repairing the financial difficulties. *Id.* at 1-2. However, the relationship continued to be strained, with disagreements in 2020 surrounding rates charged. *Id.* ¶ 16, Ex. 3. In mid-2020, Defendant Axeno began to look for other ways to operate in the United States. *Id.* ¶ 19. Defendant Axeno and four

of its executives, including Defendant Mittal, formed Defendant ADX Consulting, a Texas entity, in September 2020. *Id.* ¶ 20. Defendant ADX retained an attorney at LegalZoom for assistance with filing a trademark application in the United States. *Id.* ¶ 21. Defendant Axeno also retained two individuals at Nangia Andersen to provide advice on expanding Axeno's business in the United States independent of Plaintiffs Meyer and Zap. *Id.* ¶ 22. Defendants assert that these individuals are tax attorneys. Def. Mot. Summ. J. 7 (quoting Mittal Decl. Summ. J. ¶¶ 22-24). Plaintiffs assert that they are business consultants and strategists. Pl. Resp. 24.

On January 20, 2021, Defendant Mittal sent Plaintiff Meyer an email about the status of the parties' collaboration. Meyer Decl. Status Quo ¶ 13, Ex. G. In the email, Defendant Mittal wrote, "lately for about almost 2 years, I feel there has been lot of disagreement, difference of opinion, arguments, and friction between you and me that is giving me lot of discomfort personally and also giving me a feeling that it is not adding any benefit to the company overall and in fact inhibiting from doing business with peace of mind, and giving me lot of stress." *Id.* at 1. He also wrote, "while we will continue to support you on ongoing and any future projects (on a case to case and viability basis) that you may bring, I want to clearly steer my work independently and chart the growth path I want to put my company on. We don't have a meeting of minds on how to reach our growth goals." *Id.* at 2. Defendant Mittal then wrote, "I would like to propose that we separate our paths from being one common company to separate companies, and we should plan now is, how we will segregate our shared assets over a period of time, and settle off debts that US owes India roughly (USD 170K) in a defined period of time." *Id.*

Plaintiff Meyer states that the email led him to feel concerned about the partnership. Meyer Decl. Status Quo ¶ 13. He states, "I became concerned that I would end up in litigation with Defendants and that they would attempt to hide something." *Id.* ¶ 14. On or about January

25, 2021, he backed up the email accounts that were provided through Zap's Microsoft 365 account. *Id.* Plaintiff Meyer used Veeam Software. *Id.* ¶ 15. He also backed up Argil DX's website. *Id.* ¶ 16. Plaintiff Meyer stores the backed up emails on an external hard drive that can be plugged into any computer and accessed by a computer with Veeam software. *Id.* ¶ 17. He set up the backups to be taken automatically once per day. *Id.* ¶ 18. Plaintiffs initially disclosed that these backups included the emails of Ankur Mittal, Bushra Mehdi, Nilanjan Mukherjee, Pankaj Bansal, and Shilpi Mittal. Lang Decl. Supp. Br. ¶ 7, ECF 153.

IV. This Lawsuit

Plaintiffs Meyer and Zap sued Defendants on April 23, 2021. Compl., ECF 1. Defendant ADX Consulting waived service and moved to dismiss for failure to state a claim, which the Court granted in part and denied in part. ECF 6, 11, 27. Defendant ADX Consulting then filed an answer in December 2021. ECF 33.

In Fall 2021, Plaintiff Meyer discovered that entire email accounts had been deleted from the Microsoft 365 server. Meyer Decl. Status Quo ¶ 19. He initiated Microsoft's eDiscovery backup tool. *Id.* ¶ 20. He revoked Defendant Mittal's administrator access to the server in December 2021. *Id.* ¶ 21. On December 8, 2021, Defendant ADX Consulting's prior counsel, Susan Pitchford, contacted Plaintiffs' counsel to demand that Defendant Mittal's administrator access be restored. Harriman Decl. Opp. Summ. J. Ex. K at 16, ECF 132.

Defendants admit to deleting the emails from the Microsoft 365 server. Mittal Decl. Summ. J. ¶ 27. Defendant Mittal explains that the emails were deleted because he had established Axeno under its current name and created new email addresses for employees at the axeno.co email domain. *Id.* Defendant Axeno transferred the emails from the argildx.com domain name to the axeno.co domain server. *Id.* Defendants or their agents then deleted the

emails on the argildx.com server. *Id.* Defendants believed this was necessary to prevent Plaintiff Meyer from viewing emails they did not wish him to view. *Id.* ¶ 28. Defendant Mittal and other high-ranking employees of Defendant Axeno state that they did not grant Plaintiff Meyer access to their emails, were unaware of any policy giving him the right to do so, and were surprised to learn that he had viewed them. Mittal Decl. Summ. J. ¶¶ 33-38; Bansal Decl. Summ. J., ECF 110; Mehdi Decl. Summ. J., ECF 111; Shilpi Mittal Decl. Summ. J., ECF 112; Mukherjee Decl. Summ. J., ECF 113.

Defendants Mittal and Axeno did not appear in this case until April 2022 because of complications surrounding service of process. ECF 52. In answering the complaint, Defendants Mittal and Axeno made several counterclaims against Plaintiffs Meyer and Zap, including a claim for a violation of the SCA based on Plaintiffs' access of Defendants' emails stored on the Microsoft 365 server. Ans. to First Am. Compl. ¶¶ 349-353, ECF 59. The parties have since had several discovery disputes surrounding the emails. The Court ordered a preservation of the status quo while the issue was pending, which prevented Plaintiffs from viewing the email backups. ECF 81. As the dispute surrounding the emails progressed, Defendants filed the present motion for summary judgment on their SCA counterclaim and sanctions against Plaintiffs. The Court has since issued an order restricting Plaintiffs' right to view the disputed emails and instructing Plaintiffs to utilize the discovery process to request emails relevant to their claims and defenses. ECF 144.

After Defendants filed the present motion, Plaintiffs disclosed that the backups from the Microsoft 365 server included additional email accounts. Pl. Supp. Br., ECF 152. These include the accounts of Ashish Tripathi, Bikash Thokchom, Canh Van, Kumaresh Das, Pulkit Jan, and Rahul Kumar. Lang Decl. Supp. Br. ¶ 13. Defendants state that Ashish Tripathi and Rahul

Kumar worked in Defendant Axeno's accounting department. Def. Sur-reply 3, ECF 159. Kumaresh Das was in charge of business development. *Id.* Pulkit Jain worked in technology management. *Id.* Defendants state that Canh Van worked for Defendant ADX and did not work for Defendant Axeno. *Id.*; Mittal Decl. Sur-reply ¶ 9, ECF 160. Plaintiffs also disclosed that the backups from the server included files from Microsoft Teams, SharePoint, and OneDrive. Pl. Supp. Br. 4. Defendants state that they used those applications in their business operations. Def. Sur-reply 3-4; Mittal Decl. Sur-reply ¶¶ 5-8. Defendants represent that they "lack any concrete substantive or quantitative information" about the documents contained in Microsoft Teams, SharePoint, and OneDrive because they have not been produced in discovery. Def. Sur-reply 4.

DISCUSSION

I. Summary Judgment

Defendants move for summary judgment on their SCA violation counterclaim. Def. Mot. 1. This counterclaim alleges that Plaintiffs Meyer and Zap "intentionally accessed the Indian Defendants' private communications on an email server without authorization, or in the alternative, exceeded any authorization to access the private communications" and "obtained electronic communications while they were in electronic storage in a facility through which an electronic communication service is provided." Am. Ans. ¶¶ 350-51, ECF 99. Defendants further allege that Plaintiffs Meyer and Zap acted deliberately, willfully, intentionally, wantonly, maliciously, and oppressively. *Id.* ¶ 353. The Court concludes that Defendants are not entitled to summary judgment on this claim.

A. Standard – Summary Judgment

Summary judgment is appropriate if there is no genuine dispute as to any material fact and the moving party is entitled to judgment as a matter of law. [Fed. R. Civ. P. 56\(a\)](#). The

moving party bears the initial responsibility of informing the court of the basis of its motion, and identifying those portions of “‘the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any,’ which it believes demonstrate the absence of a genuine issue of material fact.” *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986) (quoting former Fed. R. Civ. P. 56(c)).

Once the moving party meets its initial burden of demonstrating the absence of a genuine issue of material fact, the burden then shifts to the nonmoving party to present “specific facts” showing a “genuine issue for trial.” *Fed. Trade Comm’n v. Stefanchik*, 559 F.3d 924, 927–28 (9th Cir. 2009) (internal quotation marks omitted). The nonmoving party must go beyond the pleadings and designate facts showing an issue for trial. *Bias v. Moynihan*, 508 F.3d 1212, 1218 (9th Cir. 2007) (citing *Celotex*, 477 U.S. at 324).

The substantive law governing a claim determines whether a fact is material. *Suever v. Connell*, 579 F.3d 1047, 1056 (9th Cir. 2009). The court draws inferences from the facts in the light most favorable to the nonmoving party. *Earl v. Nielsen Media Rsch., Inc.*, 658 F.3d 1108, 1112 (9th Cir. 2011). If the factual context makes the nonmoving party’s claim as to the existence of a material issue of fact implausible, that party must come forward with more persuasive evidence to support its claim than would otherwise be necessary. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

B. Standard – Stored Communications Act

The Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, governs access to stored electronic communications. At the outset the Court recognizes, along with other courts, that the SCA was enacted in the 1980s, in a very different technological environment. *E.g.*, *Matter of Warrant to Search a Certain E-Mail Acct. Controlled & Maintained by Microsoft Corp.*, 829

F.3d 197, 205-06 (2d Cir. 2016) (internal quotations omitted), *vacated and remanded on other grounds sub nom. United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018). Under the statute, a person who either “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system” is subject to liability as specified in the statute. 18 U.S.C. § 2701(a).

This provision is subject to several exceptions. As pertinent to this case, it does not apply “to conduct authorized” either “(1) by the person or entity providing a wire or electronic communications service” or “(2) by a user of that service with respect to a communication of or intended for that user.” 18 U.S.C. § 2701(c).

The statute provides for both criminal penalties and a civil action. *Id.* §§ 2701(b), 2707. To prevail in a civil action, the aggrieved party must prove that “the conduct constituting the violation [was] engaged in with a knowing or intentional state of mind.” *Id.* § 2707(a). A court may grant equitable and declaratory relief as well as damages and attorney fees. *Id.* § 2707(b). The remedies described in the statute are the exclusive remedies for violations. *Id.* § 2708.

When interpreting the SCA, courts often rely on interpretations of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030. The CFAA includes a provision covering a person who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” 18 U.S.C. § 1030(a)(2)(C). The Ninth Circuit has held that this provision and the similar SCA provision should be interpreted similarly. *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1200 (9th Cir. 2022). The Ninth Circuit has repeatedly held that the rule of lenity applies to the CFAA, even in civil cases,

because it is primarily a criminal statute. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009); *hiQ Labs*, 31 F.4th at 1200. The Court concludes that the rule of lenity applies to § 2701(a) of the SCA as well, as it is primarily a criminal provision.

i. Elements

a. Authorization

“The SCA was enacted to extend to electronic records privacy protections analogous to those provided by the Fourth Amendment.” *Matter of Warrant*, 829 F.3d 197 at 206. The Ninth Circuit has analogized the SCA to the common law of trespass. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004). Similarly, the CFAA “was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to ‘access and control high technology processes vital to our everyday lives....’” *Brekka*, 581 F.3d at 1130-31 (quoting H.R. Rep. 98–894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984)).

Neither statute defines “authorization.” The Ninth Circuit has defined “authorization” as used in the CFAA to mean “‘permission or power granted by an authority.’” *Id.* at 1133 (quoting Random House Unabridged Dictionary 139 (2001)). In the context of the CFAA, “a person uses a computer ‘without authorization’ . . . when the person has not received permission to use the computer for any purpose . . . or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.” *Brekka*, 581 F.3d at 1135. *See also United States v. Nosal*, 844 F.3d 1024, 1034 (9th Cir. 2016) (“*Nosal II*”). And “an individual ‘exceeds authorized access’ when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him.” *Van Buren v. United States*, 141 S. Ct. 1648, 1662 (2021) (interpreting the

CFAA). An individual does not violate the CFAA by accessing a computer with authorization but with an improper purpose. *Id.*

The companion *Nosal* cases from the Ninth Circuit illustrate the two means to violate the CFAA (and by extension the SCA). Nosal left his employer and then enlisted the help of former coworkers who were still at the company in starting a competing business. *United States v. Nosal*, 676 F.3d 854, 856 (9th Cir. 2012) (“*Nosal I*”). The coworkers used their employee login credentials to obtain confidential information, which they gave to Nosal. *Id.* The Ninth Circuit held that the employees did not exceed authorized access, as their employee credentials authorized them to access the information. *Id.* at 864. In *Nosal II*, the Ninth Circuit held that Nosal and his accomplices acted without authorization when, having all left the company, they used a current employee’s credentials to access company information. 844 F.3d at 1029.

b. Scierter Requirement

The mental state requirement for a civil suit under the SCA is different from the mental state requirement for a criminal prosecution. The SCA provides a cause of action where “the conduct constituting the violation is engaged in with a knowing or intentional state of mind[.]” 18 U.S.C. § 2707(a). While the cause of action provides a possibility of liability for a lesser mental state, construction of the statute should otherwise be consistent in the civil and criminal contexts. The parties disagree on the elements to which the scienter requirement attaches. Plaintiffs argue that it attaches to the access and authorization elements. Pl. Resp. 11-12. Defendants counter that it attaches only to the access element. Def. Reply 18-20, ECF 140. To determine the requisite mental state, the Court begins with the text of the statute and interprets its terms to have their ordinary meaning unless the statute indicates otherwise. *United States v. Price*, 980 F.3d 1211, 1218 (9th Cir. 2019).

In *Flores-Figueroa v. United States*, the Supreme Court interpreted a federal criminal statute covering an individual who “knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person.” 556 U.S. 646, 647 (2009) (emphasis omitted). The Supreme Court concluded that “knowingly” applied to the three verbs immediately following, as well as the phrases “without lawful authority” and “a means of identification of another person.” *Id.* at 647-48. The government conceded that the defendant must know that he or she lacked lawful authority. *Id.* at 648. The Supreme Court stated that “it seems natural to read the statute’s word ‘knowingly’ as applying to all the subsequently listed elements of the crime.” *Id.* at 650. This was because “[i]n ordinary English, where a transitive verb has an object, listeners in most contexts assume that an adverb (such as knowingly) that modifies the transitive verb tells the listener how the subject performed the entire action, including the object as set forth in the sentence.” *Id.* The Supreme Court acknowledged that proving knowledge could be difficult, but considered several examples of identity theft, including computer hacking, “types of classic identity theft where intent should be relatively easy to prove[.]” *Id.* at 656.

Accordingly, the Ninth Circuit has instructed that in determining the elements to which a scienter requirement attaches, courts should generally be guided by the “most natural grammatical meaning.” *Price*, 980 F.3d at 1218. This is not absolute. Courts should also interpret statutes to avoid absurd or unreasonable results. *Id.* For example, the Supreme Court rejected the most natural grammatical reading of a child sexual exploitation statute because it would result in convictions for individuals who did not know they were dealing with the restricted sexual materials. *Id.* (citing *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 68-70 (1994)). Courts should avoid reading in a mens rea requirement that is greater than necessary to separate otherwise innocent conduct from wrongful conduct. *Id.* at 1220. In *Price*, the Ninth Circuit held

that the mens rea of “knowingly” in a sexual assault statute applied to the element of engaging in sexual contact but not the element that such contact be without the other person’s permission. *Id.* at 1218. The Ninth Circuit concluded that a greater scienter requirement was not necessary to protect otherwise innocent actors, whereas in *Flores-Figueroa*, it was. *Id.* at 1220.

Here, the relevant SCA provision covers a person who either “intentionally accesses without authorization a facility through which an electronic communication service is provided” or “intentionally exceeds an authorization to access that facility.” 18 U.S.C. § 2701(a). The most natural reading of the statute is that “intentionally” (or, in the case of civil liability, “knowingly”) applies to the entire phrases. The grammatical structure is similar to that of the statute in *Flores-Figueroa*: an adverb denoting the required mental state followed by a transitive verb and its object. As the *Flores-Figueroa* Court pointed out, “It makes little sense to read the provision’s language as heavily penalizing a person who ‘transfers, possesses, or uses, without lawful authority’ a *something*, but does not know, at the very least, that the ‘something’ (perhaps inside a box) is a ‘means of identification.’” 556 U.S. at 650. Similarly, here the scienter requirement must attach to “facility,” because a person must either know what he or she is accessing or intend to access it. The scienter requirement must also attach to the authorization element. The second means to violate the statute illustrates this most clearly. The object of the transitive verb “exceeds” is “authorization.” 18 U.S.C. § 2701(a)(2). One cannot knowingly exceed something without knowing *what* one is exceeding—which, here, is the authorization. And it would be absurd to interpret the scienter requirement to apply to the authorization element for only the second means to violate the statute.

Further, the context of the SCA is closer to that of the identity theft statute in *Flores-Figueroa* than the sexual assault statute in *Price*. If the scienter requirement in the SCA does not

attach to the authorization element, then an individual may face liability merely for intentionally or knowingly clicking on an icon on a computer. This would sweep in situations of honest confusion that do not fit well within the statute’s purpose. The Court concludes that Congress intended the mental state requirement in the SCA to apply to the element that access be without authorization or exceed authorization.³

The illustrative cases Defendants cite are not to the contrary. An implausible claim of good faith will not exempt a bad actor from liability and may indeed fail at the summary judgment stage. *E.g.*, [Cardinal Health 414, Inc. v. Adams](#), 582 F. Supp. 2d 967, 977 (M.D. Tenn. 2008) (ex-employee “used the log-in information for *another person*, a former co-worker, to spy on the activities of his former company”); [Wyatt Tech. Corp. v. Smithson](#), No. CV05-1309 DT (RZX), 2006 WL 5668246, at *9 (C.D. Cal. Aug. 14, 2006), *aff’d in relevant part*, 345 F. App’x 236, 239 (9th Cir. 2009) (company accessed personal email account of non-employee who had never given it permission to do so); [Miller v. Meyers](#), 766 F. Supp. 2d 919, 923 (W.D. Ark. 2011) (defendant used a keylogger program to obtain plaintiff’s passwords and used them to access plaintiff’s email account).

Defendants cite a case from the Eastern District of Pennsylvania for the proposition that the Ninth Circuit’s trespass approach to the SCA forecloses any good faith defense. Def. Reply 19 (citing [Clinton Plumbing and Heating of Trenton, Inc. v. Ciaccio](#), 2010 WL 4224473, at *5 (E.D. Pa. Oct. 22, 2010) (“Because this Court has adopted the narrower [trespass analogy] view,

³ Defendants point to the presence of a good faith defense in other provisions of the SCA as evidence that Congress did not intend to allow such a defense for violations of § 2701(a). Def. Reply 19 (citing 18 U.S.C. §§ 2702(b)(8) & (c)(4); 18 U.S.C. §§ 2703(d) & (h)(2)(A)). Section 2702 addresses voluntary disclosure of communications; it dictates that a provider may not “knowingly divulge” communications and then lists exceptions where disclosure is allowed. This provision is grammatically and structurally distinct from § 2701(a). Section 2703 addresses *required* disclosures and on that basis alone is distinct from § 2701(a).

Plaintiffs need only contend that Capital One actually lacked authorization, regardless of its belief—reasonable or not—that it was authorized to access the system.”)). However, other district courts—including those on which Defendants rely elsewhere—have recognized that the trespass analogy has limits:

A big distinction between committing the tort of common law trespass and violating the SCA, of course, is that intentional conduct is required to violate the SCA, *i.e.*, a highly culpable state of mind is required. ‘Intentional’ means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person’s conscious objective.

Hahn v. Rothman, No. CV090249ODWFFMX, 2010 WL 11507395, at *3 (C.D. Cal. Oct. 8, 2010) (quoting *Cardinal Health*, 582 F. Supp. 2d at 976). The trespass analogy is useful for conceptualizing access to something in cyberspace, as opposed to physical space. It is less useful as a guide for interpreting the scienter requirement in a criminal statute. The Court concludes that the mental state element in 18 U.S.C. § 2701(a) attaches to the entire phrases in which it appears.

As a result of this statutory construction, “the well-known maxim that ‘ignorance of the law’ (or a ‘mistake of law’) is no excuse” does not preclude a defense based on lack of knowledge that one’s conduct was unauthorized. *Rehaif v. United States*, 139 S. Ct. 2191, 2198 (2019). As *Rehaif* explains, the principle “normally applies where a defendant has the requisite mental state in respect to the elements of the crime but claims to be unaware of the existence of a statute proscribing his conduct.” *Id.* (internal quotations omitted). But it “does not normally apply where a defendant has a mistaken impression concerning the legal effect of some collateral matter and that mistake results in his misunderstanding the full significance of his conduct, thereby negating an element of the offense.” *Id.* (internal quotations omitted). In *Liparota v. United States*, the Supreme Court addressed a federal statute that imposed criminal liability on “whoever knowingly uses, transfers, acquires, alters, or possesses” food stamps “in any manner

not authorized by [the statute] or the regulations.” 471 U.S. 419, 420 (1985). The Supreme Court concluded that the government had to prove that the defendant knew his use, transfer, acquisition, or possession of food stamps was unlawful. *Id.* at 425. Here, the plaintiff in an SCA claim must prove that the defendant knew that he or she was not authorized to access the facility in question or knew that the access exceeded his or her authorization.

c. Facility

The SCA does not define “facility,” but courts have established some basics. “[T]he computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users[.]” *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057 (N.D. Cal. 2012). Plaintiffs do not dispute that a Microsoft 365 cloud-based server is a facility under the SCA. Pl. Resp. 14 n.13.

d. Electronic Communication

An electronic communication is “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce,” subject to certain exceptions not relevant here. 18 U.S.C. § 2510(12) (incorporated by § 2711(1)). Emails qualify as electronic communication. *See Theofel*, 359 F.3d. at 1075.

e. Electronic Communication Service

An electronic communication service (“ECS”) is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15) (incorporated by § 2711(1)). An email system qualifies as an electronic communication service. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1057.

f. Electronic Storage

The term “electronic storage” means either “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof” or “(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17) (incorporated by § 2711(1)).

Category (A) only applies under narrow circumstances. The Ninth Circuit has indicated that it covers emails “stored on an ISP’s server pending delivery to the recipient.” *Theofel*, 359 F.3d at 1075. In the era of near-instantaneous email delivery, this subsection has limited utility.⁴ Thus, category (B) is more relevant here.

Key to category (B) is a distinction grounded in the 1980s computing environment. The SCA distinguishes an ECS from a “remote computing service” (“RCS”). *E.g.*, 18 U.S.C. § 2702(a). By its terms, the second definition of “electronic storage” applies only to ECS providers, not RCS providers. The statute defines “remote computing service” as “the provision to the public of computer storage or processing services by means of an electronic communications system.” *Id.* § 2711(2). The Senate Report accompanying the passage of the SCA provided as an example of “computer storage” that ““physicians and hospitals maintain medical files in offsite data banks.”” *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 901 (9th Cir. 2008) (quoting S. Rep. No. 99-541, at 3 (1986), U.S.C.C.A.N. 1986, 3555, 3556-57), *cert. denied USA Mobility Wireless, Inc. v. Quon*, 558 U.S. 1091 (2009).

⁴ Another district court, recognizing the outdated nature of this interpretation, concluded that unopened emails sitting in an inbox are the modern-day analogue. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 983 n.36 (C.D. Cal. 2010). The Court declines to follow this approach because *Theofel* rejected an opened-unopened email distinction. 359 F.3d at 1077.

In distinguishing an ECS from an RCS, “the key is the provider’s role with respect to a particular copy of a particular communication, rather than the provider’s status in the abstract.” Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and A Legislator’s Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1215 (2004). See also *In re U.S.*, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) (“Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself.”). In the context of email, the traditional view under the SCA is that an internet service provider (“ISP”) is a provider of ECS when an email is first sent, and a provider of RCS once the email is retrieved and stored with the ISP. Kerr, *supra*, at 1216.

The Ninth Circuit, however, has departed from this distinction and interpreted the definition of “backup” more expansively. The Ninth Circuit stated that “the lifespan of a backup is necessarily tied to that of the underlying message” and thus “[w]here the underlying message has expired in the normal course, any copy is no longer performing any backup function.” *Theofel*, 359 F.3d at 1076. See also Kerr, *supra*, at 1217. In *Theofel*, the Ninth Circuit held that emails stored on an ISP’s server after delivery qualified as backups. 359 F.3d at 1075. Whether the emails had been opened and read was irrelevant. *Id.* at 1077. *Theofel* explicitly recognized that the SCA covers different types of storage that do not fully overlap. *Id.* at 1076-77. In particular, “[a] remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes.” *Id.* at 1077.

The Ninth Circuit later held that a wireless telecommunications company providing text messaging services to a municipality was a provider of ECS and not RCS, although the company archived the text messages, because the main service provided was to facilitate communication,

not store the messages. *Quon*, 529 F.3d at 902-03. The Ninth Circuit concluded that the text messages were clearly archived as “backup protection” for the benefit of either the company or the municipality, and viewed its holding in *Theofel* as foreclosing the company’s argument to the contrary. *Id.* Accordingly, electronic communications may be in “electronic storage” as backups even if it is unclear for whom the communications are serving as backups.

g. Summary

In light of the foregoing, the Court concludes that a person violates § 2701(a) and there is a cause of action under § 2707(a) of the SCA if he or she knowingly or intentionally either (1) accesses electronic communications stored in a *facility* he or she does not have authorization to access, or (2) accesses electronic communications stored in a facility that he or she does have authorization to access, but exceeds that authorization by accessing *communications* stored within the facility that he or she does not have authorization to access. The plaintiff in an SCA claim must prove that the defendant knew that he or she was not so authorized. The communications must be in electronic storage under the particular definition of the statute. Liability is subject to the statutory exceptions. The Court now turns to those exceptions.

ii. Provider Exception

The first of the two relevant exceptions to liability under the SCA covers “conduct authorized . . . by the person or entity providing a wire or electronic communication service.” 18 U.S.C. § 2701(c)(1).

The SCA does not define “provider,” and the parties offer competing interpretations of the term. Plaintiff points to *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107 (3d Cir. 2003), *as amended* (Jan. 20, 2004). In *Fraser*, an insurance company searched an agent’s email, which was stored on the company’s main file server, after becoming concerned that the agent

might share company secrets with competitors. *Id.* at 110. The employee sued, alleging that the search violated the SCA. *Id.* at 114. The Third Circuit concluded that the employer was the provider of the service and thus could read the emails. *Id.* at 114-15. A few courts have followed or signaled agreement with this approach. See *United States v. Councilman*, 418 F.3d 67, 81 (1st Cir. 2005); *Jones v. H Grp., Inc.*, No. 3:11-CV-01012-BR, 2012 WL 195724, at *5 (D. Or. Jan. 23, 2012).

Defendants argue that the provider is the entity providing “the services to access the internet, as opposed to entities that purchase services through third parties.” Def. Resp. Opp. Status Quo 6-7, ECF 114. Defendant cites several authorities for this proposition. All involve situations in which the defendant in the SCA claim provided an email address through its domain name but stored the emails on a remote server hosted by a third party. *Conlan Abu v. Dickson*, 2021 WL 1087442, at *10 (E.D. Mich. Mar. 22, 2021), *reconsideration denied*, 2022 WL 357503 (E.D. Mich. Feb. 7, 2022) (business email accounts set up through Microsoft 365 and emails stored in the cloud on a Microsoft server); *Steinbach v. Village of Forest Park*, 2009 WL 2605283, at *5 (N.D. Ill. Aug. 25, 2009) (municipality provided email accounts but purchased internet access from a third-party provider); *Kornotzki v. Jawad*, 2020 WL 2539073, at *3 (S.D.N.Y. May 19, 2020) (business purchased email service from a third party). Several courts have also held that businesses that use the internet to sell products or services through a proprietary website are not providers of ECS. *E.g.*, *In re Jetblue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 308 (E.D.N.Y. 2005) (collecting cases).

The Ninth Circuit has addressed the meaning of “provider” as used (though not defined) in 18 U.S.C. § 2510, whose definitions the SCA incorporates. *In re App. of U.S. for an Ord. Authorizing Roving Interception of Oral Commc’ns*, 349 F.3d 1132, 1139-41 (9th Cir. 2003)

(“*Company*”). In *Company*, a business, referred to as the Company, provided on-board systems in vehicles for navigation and emergency communication. *Id.* at 1133. The systems operated through GPS and cellular technology. *Id.* Pursuant to the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, the FBI obtained court orders requiring the Company to help intercept conversations using its systems. *Id.* at 1134. The Company objected, arguing that it had no obligation to assist the FBI because it was not a provider of electronic communication services under the statute. *Id.* at 1139. The Company emphasized that it did not operate the cellular service but rather contracted with a cellular provider and then billed customers. *Id.* The Ninth Circuit rejected this argument. *Id.* It concluded that the Company was the “provider,” and the on-board system was the electronic communication service. *Id.* at 1140. It did not matter that the Company did not own or operate the cellular facilities. *Id.* The Ninth Circuit stated: “The Company’s customers are billed by the Company for the airtime and have no direct dealings with the cellular telephone company. Using the term ‘provides’ as one would in ordinary discourse, it is the Company, not the cellular telephone company, that ‘provides’ the communication service to its customers.” *Id.*

The *Company* case was decided in the context of the Wiretap Act, not the SCA, but the SCA uses the same definition of “electronic communication service.” 18 U.S.C. § 2711(1) (incorporating the definitions of § 2510). The Court concludes that the case forecloses any argument that only the underlying common carrier may be a provider of ECS. Relevant here, an entity other than an ISP may qualify as a “provider” of ECS.⁵

To clarify the types of entities that may qualify as a provider of ECS, the Court next considers § 2701 in relation to other provisions of the SCA. The SCA contains a separate

⁵ The Ninth Circuit has also held, with minimal discussion, that American Airlines was a provider of ECS through its proprietary flight reservation service. *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993).

provision restricting the ways in which “a person or entity providing an electronic communication service to the public” or a “remote computing service to the public” can divulge the contents of communications. [18 U.S.C. § 2702](#). The language “to the public” appears in [18 U.S.C. § 2702](#) but not in § 2701(c). Thus, the SCA implicitly recognizes the existence of nonpublic electronic communications providers. Kerr, *supra*, at 1220 (“Nonpublic providers can voluntarily disclose information freely without violating the SCA.”). Employers and schools are two common examples. “If a university provides accounts to its faculty and students or a company provides corporate accounts to its employees, those services are not available to the public. In these contexts, the provider offers the user an account because the provider has a special relationship with the user.” *Id.* at 1226. As another district court noted, Congress itself recognized that email systems may be public or proprietary. *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (“In describing ‘electronic mail,’ the legislative history [of the SCA] stated that ‘[e]lectronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.’”) (quoting *S. Rep. No. 99–541*, at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562).

There is good reason for the distinction. As Professor Kerr states, “These nonpublic providers generally have a legitimate interest in controlling and accessing the accounts they provide to users. Plus, their users tend to recognize that the providers will view those provider interests as more important than the privacy interests of users.” Kerr, *supra*, at 1227. The Court finds Professor Kerr’s analysis on this point compelling. It is consistent with the statutory language and structure, as well as the legislative history. It is also consistent with Ninth Circuit precedent. The act of “providing” an ECS under the SCA is not restricted to the company providing internet service or cloud storage. A business or school providing email accounts to

employees or students can also be a provider of ECS. *E.g.*, [Lindsay-Stern v. Garamszegi](#), No. SACV1401970CJCDFMX, 2016 WL 11745948, at *10 (C.D. Cal. Oct. 13, 2016) (holding that employer qualified as third-party provider of ECS for employee).

iii. User Exception

The second relevant exception to liability under the SCA covers “conduct authorized . . . by a user of that service with respect to a communication of or intended for that user.” 18 U.S.C. § 2701(c)(2). A “user” is “any person or entity who . . . uses an electronic communication service; and . . . is duly authorized by the provider of such service to engage in such use.” 18 U.S.C. § 2510(13) (incorporated by § 2711(1)). In interpreting whether conduct is “authorized,” the Court is guided by the Ninth Circuit’s directive to interpret the SCA in light of the common law of trespass. *Theofel*, 359 F.3d at 1072. In the context of trespass law, “[i]f words or conduct are reasonably understood by another to be intended as consent, they constitute apparent consent and are as effective as consent in fact.” *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1211-12 (N.D. Cal. 2014) (quoting *Restatement (Second) of Torts* § 892 in interpreting the user authorization exception to liability under 18 U.S.C. § 2701(c)(2)).

The Court also takes note of cases interpreting a related provision of the SCA. Providers of ECS to the public are restricted from divulging the contents of communications unless one of several exceptions applies, including “the lawful consent of the originator or an addressee or intended recipient of such communication[.]” 18 U.S.C. §§ 2702(a)(1), (b)(3). Other district courts in the Ninth Circuit have held that users provide consent by agreeing to an applicable privacy policy that puts the user on adequate notice that the communications may be divulged. *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 823 (N.D. Cal. 2020); *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 789 (N.D. Cal. 2019) (concluding

that California contract law governed whether consent was “lawful”). The Court believes this standard applies to § 2701(c)(2).

C. Application

Defendants have failed to show the absence of a genuine dispute as to whether Plaintiff Meyer was authorized to access Defendants’ emails.⁶ There is no dispute that Plaintiff Meyer was authorized to access the Microsoft 365 server. He cannot be liable under 18 U.S.C. § 2701(a)(1), which requires that access to the facility (the server) be without authorization. The question is therefore whether he exceeded authorization to access the server under 18 U.S.C. § 2701(a)(2), i.e., whether he was not authorized to access the portion of the server housing Defendants’ emails.⁷

i. Undisputed Matters

Several key facts are undisputed. Plaintiff Meyer originally subscribed to the Office 365 account through which the emails at issue were sent, received, and stored; and as the subscriber, he was at all times a global administrator. Defendant Mittal acquired the @argildx domain name to benefit the parties’ collaboration. It is undisputed that Plaintiff Meyer intentionally downloaded the emails. It is also undisputed that Defendant Mittal sought to terminate the parties’ collaboration and seek other opportunities in the United States in the same line of business.

⁶ The Court has identified genuine disputes of material fact that preclude summary judgment, so there is no need to address Plaintiffs’ motion for relief under Rule 56(d). *See* Pl. Resp. 7-8.

⁷ The Court’s analysis applies equally to the additional email accounts and non-email documents that Plaintiff Meyer later disclosed he had also accessed to the extent that the non-email documents are electronic communications. *See* Pl. Supp. Br. The additional emails and documents were located on the same server and accessed through the same method. Meyer Decl. Supp. Br. ¶ 10, ECF 155. It is unclear whether all of the non-email documents are electronic communications such that the SCA applies to them. The parties have not briefed the issue, and the Court will not address it further.

The Court concludes that Microsoft qualifies as a provider of ECS under the SCA by providing a Microsoft 365 subscription to Plaintiff Meyer that enabled him to send and receive emails. See *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1057 (“[T]he computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users[.]”). Plaintiffs do not dispute that a Microsoft 365 cloud-based server is a facility under the SCA. Pl. Resp. 14 n.13. Material issues of fact leave unresolved whether the emails were in electronic storage, whether Plaintiff Meyer was authorized to access the emails, and, if he was not so authorized, whether he knew that he was not authorized.

ii. Whether the Emails Were in Electronic Storage Under the SCA

Defendants have not established that the disputed emails were in electronic storage as defined by the SCA. The parties’ briefs do not address this issue, so the Court will only address it briefly. It is unclear from the record whether Defendants were storing their emails somewhere other than the Microsoft 365 server during the relevant period. See Mittal Reply Decl. ¶ 3; Mittal Decl. Summ. J. ¶ 27. The facts suggest that Microsoft may have been a provider of RCS with respect to at least some of the emails, meaning that they were not “in electronic storage” under the SCA. This is a genuine issue of fact that precludes summary judgment.

iii. Whether Plaintiff Meyer Exceeded Authorization to Access the Server

The Court evaluates several bases on which Plaintiff Meyer may have been authorized to access Defendants’ emails and concludes that there is a dispute of material fact as to whether Plaintiff Meyer exceeded authorization to access the Microsoft 365 server.

a. Authorization as Subscriber and Global Administrator

There is a genuine dispute as to whether Plaintiff Meyer's status as the account subscriber and a global administrator of the Microsoft 365 account authorized him to access the emails. Courts often rely on ECS providers' terms of service or privacy policies in determining whether access to data or communications was authorized. *E.g., In re Google, Inc. Priv. Pol'y Litig., No. C-12-01382-PSG*, 2013 WL 6248499, at *2, *12 (N.D. Cal. Dec. 3, 2013) (holding that an SCA claim against Google "border[ed] on frivolous" where Google's privacy policy authorized the challenged aggregation of data by Google); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 627 (N.D. Cal. 2021) (holding that plaintiffs failed to state a claim against Google under the SCA because Google as the provider authorized itself to collect their data). Here, if Microsoft as a provider of ECS authorized Plaintiff Meyer to access Defendants' emails because of his roles as subscriber and global administrator, the provider exception to liability may cover Plaintiff's access.

Plaintiff Meyer states, "I needed to comply with my obligations, as a Global Administrator, to monitor Affiliate Users [sic] activities on the Office 365 Account," and this was one reason he downloaded the emails. Meyer Decl. Opp. Summ. J. ¶ 19(i). It is undisputed that Plaintiff Meyer originally subscribed to the Microsoft 365 account on behalf of Zap and that he was a global administrator at all relevant times. The Microsoft Online Subscription Agreement informs the subscriber: "You control access by End Users, and you are responsible for their use of the Product in accordance with this agreement." Williams Decl. Opp. Summ. J. Ex. G at 2. An End User is "any person you permit to access Customer Data hosted in the Online Services or otherwise use the Online Services[.]" *Id.* at 10. In the words of Microsoft, global administrators "have almost unlimited access to [the] organization's settings and most of its

data.” *Id.* Ex. H at 2. It appears that Defendant Mittal and other Axeno employees may qualify as end users and that Plaintiff Meyer may have had considerable control over their access to and use of the Microsoft services provided through the subscription.⁸

Defendant Mittal states in his declaration that “Global Admins do not have the ability to directly access or read emails of other users.” Mittal Decl. Summ. J. ¶ 15. Plaintiffs object that this statement is inadmissible because Defendant Mittal has not qualified himself as an expert in Microsoft 365. Pl. Resp. 6 n.8. The Court agrees that the statement as phrased is an improper lay opinion and thus should not be considered. *See Fed. R. Evid. 701; Smith v. Pac. Bell Tel. Co.*, 649 F. Supp. 2d 1073, 1088 (E.D. Cal. 2009) (sustaining objection to statement in affidavit that affiant had advised that a GPS was unreliable where the affiant had not established qualifications to opine on the reliability of a GPS). That said, the description from Microsoft standing alone does not make it clear whether and how a global administrator can access email accounts of other users, and when such access would be necessary. The Court cannot conclude on the record before it that Plaintiff Meyer was or was not authorized as a subscriber and global administrator to access Defendants’ emails. This unresolved issue precludes summary judgment.

Defendants argue that “[i]t is no defense that a party has administrator privileges to the account.” Def. Mot. Summ. J. 17. Defendants rely on a trio of cases from other circuits, and the Court finds none of them compelling on that point. The first case is *Hamilton Grp. Funding, Inc. v. Basel*, 311 F. Supp. 3d 1307 (S.D. Fla. 2018). In finding the defendant liable under the SCA, the district court relied on then-binding Eleventh Circuit precedent interpreting “exceeds

⁸ Pointing to Plaintiff Meyer’s deposition testimony, Defendants argue that the server was jointly owned. Def. Reply 13-14. It is also undisputed that Plaintiff Meyer originally subscribed to Microsoft 365 on behalf of Zap, and the record does not reflect a change in the subscriber identity. Further, as discussed below, the existence of the partnership is disputed. It is unclear from this record which entities held a property interest in the server.

authorized access” in the CFAA. *Id.* at 1317. In *Van Buren*, the Supreme Court squarely rejected the Eleventh Circuit’s interpretation. 141 S. Ct. at 1662. *Hamilton* is not good law. The second case is *Joseph v. Carnes*, 2013 WL 2112217 (N.D. Ill. May 14, 2013), which addressed a motion to dismiss. More relevant here, the district court later denied the defendants’ motion for summary judgment over fact issues surrounding their right to access the plaintiff’s email account, which they had accessed through an email archiving program. 108 F. Supp. 3d 613, 616-17 (N.D. Ill. 2015). Similarly, in *Conlan Abu v. Dickson*, the court found that there was a genuine dispute as to whether defendants’ access was authorized. 2021 WL 1087442, at *7 (E.D. Mich. Mar. 22, 2021), *reconsideration denied*, 2022 WL 357503 (E.D. Mich. Feb. 7, 2022).

Defendants also point to a June 2017 text conversation between Plaintiff Meyer and Defendant Mittal as evidence that a global administrator cannot access other users’ email accounts. Def. Reply 1-2. However, this conversation is inconclusive. First, Defendant Mittal stated that he did not feel comfortable with another Zap employee accessing his emails. Mittal Reply Decl. Ex. 32. He did not state that he did not feel comfortable with Plaintiff Meyer viewing his emails, despite knowing that Plaintiff Meyer was a global administrator. Defendant Mittal stated that the Zap employee should be told to seek approval before accessing either Defendant Mittal’s or Plaintiff Meyer’s account. *Id.* This could reasonably be interpreted as a desire to protect executives’ emails from employee access. Second, Plaintiff Meyer explained, “I cannot impersonate anyone unless I go into administration and set it up for each user that I want to be able to impersonate.” *Id.* This statement suggests that global administrators *do* have the ability to access users’ emails. Lacking explanation of the technology and processes involved, the Court cannot determine the scope of a global administrator’s access to email accounts. And there is no evidence that Plaintiff Meyer and Defendant Mittal agreed that their emails either

would or would not be private from each other.⁹ There is a genuine dispute as to whether Plaintiff Meyer as a global administrator and/or subscriber of the Microsoft 365 account was authorized to access Defendants’ emails.

b. Authorization as Partner of Argil DX

There is a genuine dispute as to whether the partnership “Argil DX” was formed between Plaintiff Meyer and Defendant Mittal, and possibly their respective businesses. There is also a genuine dispute as to whether Plaintiff Meyer could access Defendants’ emails stored on the Microsoft 365 server in order to protect the partnership.

1. Existence of Partnership

Plaintiff has established a genuine dispute as to whether the collaboration known as Argil DX was a partnership. Under Oregon law, “the association of two or more persons to carry on as co-owners a business for profit creates a partnership, *whether or not the persons intend to create a partnership.*” O.R.S. 67.055(1) (emphasis added). The statute lists five non-exclusive factors to consider in determining whether two or more persons created a partnership:

- (A) Their receipt of or right to receive a share of profits of the business;
- (B) Their expression of an intent to be partners in the business;
- (C) Their participation or right to participate in control of the business;
- (D) Their sharing or agreeing to share losses of the business or liability for claims by third parties against the business; and
- (E) Their contributing or agreeing to contribute money or property to the business.

O.R.S. 67.055(4)(a). “The sharing of gross returns does not by itself create a partnership, even if the persons sharing them have a joint or common right or interest in property from which the returns are derived.” O.R.S. 67.055(4)(c). “It is a rebuttable presumption that a person who

⁹ Although the reasonable expectation of privacy standard of the Fourth Amendment is not part of an SCA claim, to the extent that it is relevant, the Court would not conclude as a matter of law that Defendants had an objectively reasonable expectation of privacy in their emails.

receives a share of the profits of a business is a partner in the business, unless the profits were received in payment of . . . [w]ages or other compensation to an employee or independent contractor[.]” O.R.S. 67.055(4)(d)(B). But “[a]n agreement to share losses by the owners of a business is not necessary to create a partnership.” O.R.S. 67.055(4)(e). Both natural persons and business organizations may form a partnership. *E.g.*, [*Wirth v. Sierra Cascade, LLC*, 234 Or. App. 740, 747, 230 P.3d 29 \(2010\)](#) (partnership between three natural persons and one LLC).

There is evidence for at least three of the five factors pointing to the formation of a partnership. Defendant Mittal wrote to Plaintiff Meyer after a business meeting: “I think it’s just a beginning of a new journey of our partnership so looking forward to this journey.” Meyer Decl. Opp. Summ. J. ¶ 10, Ex. P. The parties created a website for Argil DX that announced a “merger” of Plaintiff Meyer and Defendant Mittal’s businesses. *Id.* ¶ 11, Ex. Q at 1. The parties also created a social media presence for Argil DX. *Id.* ¶ 12, Exs. S, W, U. On social media, their website, and their organizational chart, the parties referred to Plaintiff Meyer as President and CEO and Defendant Mittal as President. *Id.* ¶ 12, Exs. R, S, T, U, W. Defendant Mittal acquired the domain name @argildx as part of the parties’ efforts. Mittal Decl. Summ. J. ¶ 8. Plaintiff Meyer allowed Zap’s Office 365 account to be used for email accounts within that domain. Meyer Decl. Opp. Summ. J. ¶ 8. The parties then split the costs of the account. *Id.* Plaintiff Meyer added Defendant Mittal as a global administrator. Mittal Decl. Summ. J. ¶ 15. Emails between Plaintiff Meyer and Defendant Mittal show high-level discussions about the overall direction of the business. Mittal Decl. Summ. J. Exs. 3, 5. This evidence shows that factors (B), (C), and (E) support the finding that the parties formed an oral partnership.

The evidence is less clear with respect to factors (A) and (D), the allocation of profits and losses. Plaintiff Meyer states that the parties had a system for calculating revenues from projects

and sharing profits. Meyer Decl. Opp. Summ. J. ¶ 14. There is little documentation to reinforce his declaration. At least one email shows that Plaintiff Meyer and Defendant Mittal talked about profit sharing. Mittal Decl. Summ. J. Ex. 3. Emails between Plaintiff Meyer and Defendant Mittal suggest that Plaintiff Meyer was prepared to contribute funds to assist the Indian side of the business during a financially difficult period. Mittal Decl. Summ. J. Ex. 5 at 2.

Defendants submit evidence that points against the formation of a partnership. Plaintiff Meyer conceded that he and Defendant Mittal did not sign any documentation memorializing the purported merger. Meyer Dep. I 48:9-18. Plaintiff Meyer did not recall discussing additional rights or obligations for their respective businesses, or governing law or taxation for the partnership. *Id.* at 58:17-25, 60:17-61:7. The parties generally agreed that the businesses would handle personnel matters for their own employees. *Id.* at 63:8-64:6.¹⁰ Federal tax returns Plaintiff Meyer submitted for Plaintiff Zap for 2017 through 2021 indicated that Zap did not own an interest in a partnership. Aldred Reply Decl. ¶¶ 7-8, Exs. 39-43.

Ultimately, at this stage, the Court is to construe all evidence in the light most favorable to Plaintiffs and seek the existence of a genuine dispute of material fact. Plaintiffs' evidence clears this hurdle. Viewing the facts in the light most favorable to Plaintiffs, the general partnership Argil DX existed, and Plaintiff Meyer and Defendant Mittal were partners. Zap and Axeno (then Accunity) may also have been partners.

¹⁰ Defendants point to a statement by Plaintiff Meyer that the partnership did not directly have its own employees. Aldred Reply Decl. Ex. 33, Meyer Dep. I at 122:14-24. Defendants assert that the Axeno executives were not employees of Meyer, Zap, or the partnership. Def. Reply 11. However, it is a question of law whether Axeno employees were employees of any partnership or were independent contractors, the theory Defendants favor. *Moholt v. Dooney & Bourke, Inc.*, 63 F. Supp. 3d 1289, 1304 (D. Or. 2014) (“Whether an individual is an employee or an independent contractor is a legal conclusion.”) (quoting *Schaff v. Ray's Land & Sea Food Co.*, 334 Or. 94, 99, 45 P.3d 936 (2002)).

2. Authorization to Access Emails

There is a genuine dispute as to whether Plaintiff Meyer had the right to access Defendants' emails by virtue of his position as a partner of Argil DX. Several provisions of the Oregon partnership statute are implicated here, and they point in different directions in this case.

"Each partner has equal rights in the management and conduct of the partnership business." O.R.S. 67.140(7). "Each partner is an agent of the partnership for the purpose of its business." O.R.S. 67.090(1). A partner's act in the ordinary course of business will generally bind the partnership, while an act outside the ordinary course of business will only bind the partnership if the other partners authorized that act. O.R.S. 67.090(1)-(2). It is a question of fact whether a partner acts within the scope of partnership business. *Nicolai-Neppach Co. v. Abrams*, 116 Or. 424, 429, 240 P. 870 (1925).

"A partnership is liable for loss or injury caused to a person, including a partner, or for a penalty incurred as a result of a wrongful act or omission or other actionable conduct of a partner acting in the ordinary course of business of the partnership or with authority of the partnership." O.R.S. 67.100(1). In general, "all partners are liable jointly and severally for all obligations of the partnership unless otherwise agreed by the claimant or provided by law." O.R.S. 67.105(1).

"The only fiduciary duties a partner owes to the partnership and the other partners are the duty of loyalty and the duty of care[.]" O.R.S. 67.155(1). The duty of loyalty includes (a) accounting for any profit or property due to the partnership, including partnership opportunities, (b) refraining from dealing with the partnership in a manner adverse to its interests, and (c) refraining from competing with the partnership before it dissolves. O.R.S. 67.155(2). The duty of care "is limited to refraining from engaging in grossly negligent or reckless conduct, intentional misconduct or a knowing violation of law." O.R.S. 67.155(3). The duties of loyalty and care are

to be discharged “consistent with the obligation of good faith and fair dealing.” O.R.S.

67.155(4). Partners owe fiduciary duties to each other and the partnership even when the relationship is strained or conditions arise that might justify dissolution of the partnership.

Delaney v. Georgia-Pac. Corp., 278 Or. 305, 310, 564 P.2d 277, *supplemented*, 279 Or. 653, 569 P.2d 604 (1977).

Plaintiff Meyer states that he accessed the emails for “legitimate business reasons.” Meyer Decl. Opp. Summ. J. ¶ 19. These reasons include (1) the risk of liability for wrongful acts by employees or independent contractors with apparent authority to act on behalf of the partnership; (2) the need to protect the partnership from misappropriated business opportunities; and (3) to comply with his obligations as global administrator to monitor affiliate users’ activities on the Office 365 account. *Id.* Plaintiff Meyer also testified in his deposition that he was concerned about losing partnership intellectual property contained in the emails. Williams Decl. Opp. Summ. J. Ex. A, Meyer Dep. II 260:9-12.

Oregon partnership law and evidence in the record support Plaintiff Meyer’s declaration. First, under Oregon law, Plaintiff Meyer could be liable as a partner for acts taken by others apparently on behalf of the partnership. O.R.S. 67.105(1). Second, it is undisputed that Defendants Mittal and Axeno sought to pursue opportunities in the United States in the same line of business independent of their collaboration with Plaintiffs Meyer and Zap, and that Defendant Mittal advised Plaintiffs of this intention. Plaintiff Meyer could have reasonably believed that partnership opportunities would be misappropriated or that partnership intellectual property could be lost. *See Liggett v. Lester*, 237 Or. 52, 58-59, 390 P.2d 351 (1964) (partner must obtain consent of other partners to engage in a competitive enterprise). The Court previously addressed Plaintiff Meyer’s third reason, which may also have merit.

On the other hand, as Defendants argue, the evidence in the record suggests that Plaintiff Meyer's act of downloading the emails in January 2021 was not an act in the ordinary course of business. At his deposition, Plaintiff Meyer admitted that prior to 2021, he did not regularly download emails from other accounts in the @argildx domain. Aldred Reply Decl. Ex. 50, Meyer Dep. II 257:3-258:21. Plaintiff Meyer stated that he started taking the backups after receiving an email from Defendant Mittal that led him to be concerned about the state of the partnership. Meyer Decl. Status Quo ¶¶ 13-14. Thus, if Defendant Mittal was still a partner, it may be that Plaintiff Meyer needed his approval to start taking the backups. The record suggests that Defendant Mittal was still a partner. His January 20, 2021, email to Plaintiff Meyer served as notice of his intent to withdraw from the partnership, but it did not necessarily serve as an actual withdrawal, as Defendant Mittal stated that he would continue to work on existing projects. Meyer Decl. Status Quo Ex. G. See *Timmermann v. Timmermann*, 272 Or. 613, 624-25, 538 P.2d 1254 (1975) (holding that an at-will partnership did not dissolve when one of the partners expressed an intent to leave but rather when he stopped participating in partnership business). Plaintiff Meyer provides no evidence that Defendant Mittal approved the taking of the backups, or indeed that he was aware of Plaintiff Meyer's decision to begin taking the backups.

The Oregon partnership statute thus provides support for Plaintiffs' position and Defendants' position. The Court did not find any cases clarifying whether, when a partner reasonably believes that another partner breached his or her fiduciary duties to the partnership, that partner may take certain measures to protect the partnership and its property, including retention of business emails. The Court concludes that there is a genuine dispute as to whether Plaintiff Meyer could access Defendants' emails in order to protect the partnership.

c. Authorization as Provider of ECS

There is also a genuine dispute as to whether Plaintiffs Meyer and Zap were providers of an electronic communications service. There are three levels of actors with respect to the @argildx email accounts at issue. First, Microsoft provided a subscription to its Office 365 email service, which included cloud storage. Second, Plaintiff Meyer, acting on behalf of Zap, paid for that subscription and used it to create email accounts in the @argildx domain name. Third, employees of Axeno were assigned email addresses with the @argildx domain name. It follows that two levels of authorization were required for Axeno employees to use their email accounts: Microsoft authorized Plaintiffs to use its services, and Plaintiffs in turn authorized the employees to use email accounts associated with Plaintiffs' Microsoft 365 account.

Viewing the facts in the light most favorable to Plaintiffs, the Court concludes that Plaintiffs Meyer and Zap may qualify as providers of ECS under the SCA. In his capacity as president of Zap, Plaintiff Meyer created, administered, and paid for the Microsoft 365 account. Meyer Decl. Opp. Summ. J. ¶¶ 7-8. Plaintiff Meyer had to authorize the creation of @argildx email addresses and assign them to others, including employees of Zap and Axeno, and including Defendant Mittal. Plaintiff Meyer as the subscriber and original global administrator chose to make Defendant Mittal a global administrator, and Defendants Mittal and Axeno reimbursed him for a portion of the subscription fees. *Id.* ¶¶ 8-9; Mittal Decl. Summ. J. ¶ 15; Meyer Decl. Status Quo ¶ 9.

The facts here are comparable to the *Company* case discussed above, where the business providing on-board vehicle navigation and communication systems did not provide cellular service, but contracted with a cellular provider and then billed its customers, who did not deal directly with the cellular company. [Company](#), 349 F.3d at 1139-40. Plaintiff Meyer contracted

with Microsoft for email services and cloud storage, and then billed Defendant Axeno for a portion of the fees for using the account. Defendant Axeno did not have its own account with Microsoft.

The Court does not find it material that the emails were stored on Microsoft's servers in the cloud rather than a local server belonging to Zap. The exception at [18 U.S.C. § 2701\(c\)\(1\)](#) turns on whether Plaintiffs Meyer and Zap are providers of an ECS, not on whether they are a facility through which ECS is provided. See *In re iPhone Application Litig.*, 844 F. Supp. 2d at [1058](#) (distinguishing “provider” and “facility”). An ECS is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” [18 U.S.C. § 2510\(15\)](#). By creating email accounts for others using the @argildx domain name on Zap's Microsoft 365 account, Plaintiff Meyer gave the individuals with the assigned email addresses the ability to send and receive emails.

Subscribing to Microsoft 365 entitles the subscriber to a certain amount of storage space on Microsoft's servers. By creating and paying for a Microsoft 365 account for Zap, Plaintiff Meyer was entitled to a certain amount of storage space on Microsoft's servers for emails sent from and received by the associated email addresses. The Court sees nothing in the definition of ECS that restricts providers of ECS to those entities that also own or operate the physical equipment. The Ninth Circuit's decision in the *Company* case indicates that no such restriction exists. [349 F.3d at 1139-40](#) (holding that provider of on-board vehicle communication systems was a provider of ECS despite not owning or operating cellular facilities, and analogizing to a long-distance phone carrier paying a local carrier to use its phone lines). In sum, there is a genuine dispute as to whether Plaintiff Meyer was authorized to access the disputed emails because of the provider exception.

d. Authorization by User Consent

There is also a genuine dispute as to whether the user authorization exception applies. Defendant Mittal and other high-level executives at Defendant Axeno assert that they did not directly authorize Plaintiff Meyer to access their emails and were not presented with any policy authorizing Plaintiff Meyer to access their emails. Mittal Decl. Summ. J. ¶¶ 33-38; Bansal Decl. Summ. J.; Mehdi Decl. Summ. J.; Shilpi Mittal Decl. Summ. J.; Mukherjee Decl. Summ. J. Plaintiff Meyer does not assert that Defendants expressly authorized him to access the emails. Nor does he allege the existence of any partnership policy authorizing him to access the emails. The record reflects no policy or agreement about email access beyond an assurance from Plaintiff Meyer to Defendant Mittal that one particular Zap employee with administrator privileges would need to seek permission before accessing others' email accounts. Mittal Reply Decl. ¶ 3, Ex. 32.

Instead, Plaintiffs suggest that Defendants provided their consent for Plaintiff Meyer to view their emails by agreeing to the Microsoft terms of service, which they argue incorporate the privacy statement. Pl. Resp. 18. Microsoft's privacy statement, as updated in December 2022, contains the following language:

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account, that organization can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of a change of employment, for example), you may lose access to the products and content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Williams Decl. Opp. Summ. J. Ex. E at 15. The privacy statement also says that use of Microsoft products is subject to the organization's policies and that data processing is subject to a contract between Microsoft and the organization. *Id.*

The Microsoft services agreement states: "If you received your Microsoft account from a third party, the third party may have additional rights over your account, like the ability to access or delete your Microsoft account." *Id.* Ex. C at 5. It follows this with "Please review any additional terms the third party provided you, as Microsoft has no responsibility regarding these additional terms." *Id.* It also provides that account credentials cannot be transferred to another user or entity. *Id.* The terms of service state that if a user signs in with a work or school email address, the user (referred to as "you") "agree that the owner of the domain associated with your email address" may "control and administer your account, and access and process your Data, including the contents of your communications and files[.]" *Id.* at 6. The terms of service as updated in June 2022 also contain these terms. *Id.* Ex. D at 6, 7.

Defendants counter that the privacy statement is not a contract and is not incorporated into the terms of service, and further that it does not grant an employer any rights but rather describes what an employer "may be *technically capable* of doing." Def. Reply 21. In discussing the privacy statement, Microsoft's terms of service state: "Where processing [of data] is based on consent and to the extent permitted by law, by agreeing to these Terms, you consent to Microsoft's collection, use and disclosure of Your Content and Data as described in the Privacy Statement. In some cases, we will provide separate notice and request your consent as referenced in the Privacy Statement." Williams Decl. Opp. Summ. J. Ex. C at 3, Ex. D at 4. This language suggests that the privacy statement *is* incorporated into the terms of service.

Further, the language in the terms of service themselves is sufficient to raise the issue of Defendants' consent to Plaintiff Meyer's access of their emails. Defendants appear to concede that the terms of service are a contract. Def. Reply 21. The terms of service provide that an individual consents to them by using the services. Williams Decl. Opp. Summ. J. Ex. C at 3, Ex. D at 4. Defendants do not argue that the terms of service did not apply to the relevant Axeno employees at the relevant times. The question, then, is whether the terms of service provide a basis to establish that these Axeno employees consented to Plaintiff Meyer's access of their emails.

On the record before it, the Court cannot determine whether a user grants an employer permission to access his or her emails by agreeing to the Microsoft terms of service. The provisions above do appear to constitute agreement to such access. This issue is closely intertwined with the Court's earlier discussion of global administrator and subscriber access to the emails. The original subscriber to Microsoft 365 (who is automatically a global administrator) is required to monitor end users, and has access to almost all data as a global administrator; it is unclear whether this includes access to emails of end users. If it does, it follows that the terms of service would most reasonably be interpreted to advise employees that their employer as the subscriber to the service can access their emails. Agreeing to the terms of service (by using Microsoft services) would constitute an acknowledgment that employers may view employee emails. As discussed above, the nature of the employment relationship between Plaintiffs Meyer and Zap and Defendants Mittal and Axeno and employees of Defendant Axeno is uncertain.

Defendants point to the following language in the terms of service: "these Terms are solely for your and our benefit; they aren't for the benefit of any other person, except for

Microsoft’s successors and assigns.” Williams Decl. Opp. Summ. J. Ex. D at 28. They suggest that such language means that the terms of service do not grant employers the right to view employee emails. Def. Reply 21. However, if another agreement (i.e., the Microsoft 365 subscription agreement) requires the subscriber to monitor content of end users, the terms of service would not grant any rights. Rather, in using the Microsoft services and thereby agreeing to the terms of service, an employee who is an end user agrees to the employer’s exercise of rights bestowed on the employer by a different contract with Microsoft. In short, the terms of service may serve a notice and consent function. As the scope of the subscriber’s duties and a global administrator’s right of access has not been clarified, the issue of user consent through the terms of service cannot be resolved on this record. There is a material dispute as to whether Defendant Mittal and other employees of Defendant Axeno granted Plaintiff Meyer permission to access their emails.

iv. Whether Plaintiff Meyer Knew He Exceeded Authorization

Assuming for the sake of argument that Plaintiff Meyer exceeded his authorization to access the server when he downloaded the emails, there is a genuine dispute as to whether he knew he was not so authorized. Plaintiff Meyer states that he accessed the emails for “legitimate business reasons.” Meyer Decl. Opp. Summ. J. ¶ 19. He listed three reasons: (1) the risk of liability for wrongful acts by employees or independent contractors with apparent authority to act on behalf of the partnership; (2) the need to protect the partnership from misappropriated business opportunities; and (3) to comply with his obligations as global administrator to monitor affiliate users’ activities on the Office 365 account. *Id.* As discussed above, there are facts in the record supporting these concerns as legitimate. Plaintiff Meyer also testified that he did not believe he needed to talk to anyone at Axeno about backing up the emails because he was the

CEO. Williams Decl. Ex. A, Meyer Dep. II 260:13-17. If Plaintiff Meyer was mistaken about his rights as a partner or CEO, this mistake was as to a collateral matter, not the SCA itself, so it would negate the mental state required to find that he violated the SCA. *Rehaif*, 139 S. Ct. at 2198. Plaintiff Meyer’s credibility is for the jury to assess.

Defendants point out that Plaintiff Meyer does not assert that he directly sought permission from them to access the emails, and that he used a means of access that would not alert Defendants to his activities. Def. Reply 2-3. Defendants also note that Plaintiff Meyer admitted that he was considering filing a lawsuit against Defendant Axeno. *Id.* at 4. Assuming these facts are true and viewing them in the light most favorable to Plaintiffs, Plaintiff Meyer could have been legitimately motivated by the need to protect the partnership and believed that filing a lawsuit against Defendants was the best means to do so. Given that Defendant Mittal had recently emailed Plaintiff about his intention to end their collaboration and pursue other business opportunities, Plaintiff Meyer could reasonably believe that downloading the emails was necessary to preserve them before litigation and to protect partnership intellectual property.

Defendants cite several cases for the proposition that a protestation of good faith may be insufficient to defeat a finding that someone acted knowingly or intentionally. Def. Reply 15. The Court agrees that such situations exist. For example, where an ex-employee “used the log-in information for *another person*, a former co-worker, to spy on the activities of his former company,” his conduct was plainly unauthorized. *Cardinal Health*, 582 F. Supp. 2d at 977. Under those circumstances, it was implausible for the defendant to argue that he thought his conduct was authorized. *See id.* In the case before this Court, Plaintiff Meyer was the subscriber to Microsoft’s services, the original global administrator, and, viewing the facts in the light most favorable to him, a partner in a partnership whose other partner had just told him he intended to

leave the partnership and pursue other opportunities in the same line of business. Under these circumstances, Plaintiff Meyer's belief that he could access the portion of the server housing Defendants' emails in order to protect the partnership is not facially implausible. Questions of fact about his mental state preclude summary judgment.

Defendants are not entitled to summary judgment on their SCA claim. The Court now turns to Defendants' motion for sanctions.

II. Sanctions

Defendants move for several sanctions: dismissal of all of Plaintiffs' causes of action with prejudice, exclusion of all of the disputed emails and evidence derived from them, an order that Plaintiffs destroy the disputed emails, and payment of Defendants' attorney fees and costs. Def. Mot. Summ. J. 1. The Court declines to sanction Plaintiffs.

A. Standard

A federal court has the inherent power to impose sanctions on a party to litigation. *Chambers v. NASCO, Inc.*, 501 U.S. 32, 43 (1991). In doing so, the court should carefully exercise its discretion "to fashion an appropriate sanction for conduct which abuses the judicial process." *Id.* at 44-45. "A district court may, among other things, dismiss a case in its entirety, bar witnesses, exclude other evidence, award attorneys' fees, or assess fines." *Am. Unites for Kids v. Rousseau*, 985 F.3d 1075, 1088 (9th Cir. 2021).

An individual subject to sanctions is entitled to procedural protections. *Id.* at 1088-89. Civil procedures apply to sanctions that are remedial or compensatory, while criminal procedures apply to punitive sanctions. *Id.* at 1089. A sanction is compensatory where it is tailored to the specific harm caused by the sanctionable misconduct. *Id.* The court must find that the sanctionable misconduct was a "but-for" cause of the harm. *Id.* at 1089-90.

“When acting under its inherent authority to impose a sanction, as opposed to applying a rule or statute, a district court must find either: (1) a willful violation of a court order; or (2) bad faith.” *Id.* at 1090. Only the latter is at issue here. To impose sanctions based on bad faith, the court must “make an explicit finding that the sanctioned party’s conduct constituted or was tantamount to bad faith.” *Id.* (internal quotations omitted). Bad faith may be found where conduct was “done vexatiously, wantonly, or for oppressive reasons.” *Id.* This includes actions in the conduct of the litigation. *Id.* For example, defendant Goodyear Tire & Rubber Co. acted in bad faith where it withheld relevant test results for its tires from plaintiffs who sued the company after getting into vehicle accidents. *Goodyear Tire & Rubber Co. v. Haeger*, 581 U.S. 101, 105 (2017).

B. Application

The genuine disputes of material fact in this case demonstrate that sanctions are not appropriate. The Court declines to find at this time that Plaintiff Meyer acted in bad faith. Given the uncertainty surrounding whether Plaintiff Meyer was authorized to access the emails, the Court declines to find that his conduct was vexatious, wanton, or oppressive. Plaintiff Meyer provided legitimate business reasons for accessing the disputed emails. Meyer Decl. Opp. Summ. J. ¶ 19. They center on an intent to protect the putative partnership after Defendant Mittal advised of his intention to end the parties’ collaboration and pursue other opportunities in the same line of business. The Court rejects Defendants’ contention that Plaintiff Meyer’s desire to sue them was necessarily a nefarious motive. Because the record does not establish at this time that Plaintiff Meyer acted in bad faith, sanctions are not appropriate.¹¹

¹¹ Defendants argue that Plaintiffs’ disclosure that Plaintiff Meyer accessed additional emails and non-email documents strengthens the case for sanctions. Def. Sur-reply. There is still a genuine dispute as to whether Plaintiff Meyer acted in good faith to protect the partnership, so the Court

Defendants assert that violations of the SCA, the CFAA, and Oregon's computer crime statute justify an imposition of sanctions. Def. Mot. Summ. J. 16-20. There is a genuine dispute as to whether Plaintiff Meyer violated the SCA, and sanctions are not warranted based on an unproven violation of the SCA. The Court rejects alleged violations of the CFAA and Oregon law as a basis for sanctions. Defendants did not assert claims under these statutes in their answer, and they provide minimal analysis of the statutory language or application of it to the facts.¹²

Defendants point to many cases in which a party was sanctioned for inappropriately obtaining documents during or in anticipation of litigation. Def. Mot. Summ. J. 21-23. These cases generally involve terminated employees who improperly obtained company documents. *E.g.*, *Fayemi v. Hambrecht & Quist, Inc.*, 174 F.R.D. 319, 321 (S.D.N.Y. 1997) (plaintiff in employment discrimination case entered company offices after termination and obtained information from his former supervisor's computer files); *Jackson v. Microsoft Corp.*, 211 F.R.D. 423, 425-26 (W.D. Wash. 2002) (plaintiff in employment discrimination case either stole or purchased from another employee two CDs containing emails from his supervisor's computer and then lied to the court about it); *Ashman v. Solelectron Corp.*, 2008 WL 5071101, at *2 (N.D. Cal. Dec. 1, 2008) (terminated employee logged on to employer's network and read emails of high-level managers); *Lynn v. Gateway Unified Sch. Dist.*, 2011 WL 6260362, at *2 (E.D. Cal. Dec. 16, 2011) (terminated employee made a copy of all emails on the defendant's server). The

continues to conclude that sanctions are not appropriate. The Court acknowledges Defendants' frustration with the course of Plaintiffs' responses during discovery, *id.* at 2-5, but Defendants' motion for sanctions is based on Plaintiff Meyer's access of the disputed emails and non-email documents, not possible discovery violations. Plaintiffs' ability to view the disputed emails has been restricted by orders of this Court, and the Court declines to infer that Plaintiff Meyer acted in bad faith in downloading the emails based on Plaintiffs' conduct in discovery.

¹² Defendants concede that they cannot satisfy the minimum loss requirement to state a claim under the CFAA. Def. Mot. Summ. J. 19 n.7.

Court does not find these cases instructive. As the above discussion of Defendants’ SCA claim illustrates, leadership at a business may have greater authorization to view employees’ communications sent using work accounts. Plaintiff Meyer’s conduct was not facially illegal.

Defendants also rely on *Gates v. Wheeler*, 2010 WL 4721331 (Minn. Ct. App. Nov. 23, 2010), which involved co-owners of an LLC rather than an employer and employee. In *Gates*, one co-owner of the LLC enlisted the help of an information technology officer at the company to access the other owner’s email account and have all emails routed to him. *Id.* at *6. The *Gates* decision focuses primarily on the plaintiff’s state-law invasion of privacy claim, which relies on a different standard, and only briefly mentions the SCA. *Id.* *Gates* is factually and legally distinct, and the Court does not find it persuasive.

Defendants express concerns about Plaintiffs’ alleged reliance on privileged documents contained in the email backups. Def. Mot. Summ. J. 28. Plaintiffs counter that this is a “red herring,” arguing that the attorney-client privilege has not been established for any documents or that, if the documents were privileged, any privilege has been waived. Pl. Resp. 24.¹³ Defendants focus on a proposal prepared by two individuals at Nangia Andersen (“the Nangia proposal”). Def. Mot. Summ. J. 34. The Court has since ruled that the Nangia proposal is not privileged. Op. & Ord., ECF 163. Claims of privilege will continue to be handled through the discovery process.

Defendants have failed to convince the Court at this time that Plaintiff Meyer’s conduct was wrongful as a matter of law. When wrongdoing is uncertain, sanctions are not appropriate. The Court declines to dismiss Plaintiffs’ causes of action, exclude the evidence from the emails,

¹³ Defendants argue that waiver is not a defense to sanctions. Def. Reply 23. The Court construes Plaintiffs’ argument, Pl. Resp. 23-24, as addressing whether Defendants waived the right to assert the attorney-client privilege, not whether Defendants waived the right to move for sanctions.

or order Plaintiffs to destroy documents in their possession. This does not leave Defendants without remedy. If Defendants prevail on their SCA claim—or their invasion of privacy claim—at trial, they will have a right to damages. Further, the Court has instituted measures to protect Defendants by requiring Plaintiffs to seek documents through discovery rather than viewing the disputed emails. Order, ECF 144.

III. Attorney Fees

Defendants seek attorney fees based on their SCA counterclaim and the Court’s inherent power to impose sanctions. Def. Mot. Summ. J. 30. Neither basis applies because Defendants have not prevailed on their SCA claim and the Court declines to find that Plaintiff Meyer acted in bad faith. An award of attorney fees is not appropriate at this time.

IV. Discovery of Plaintiffs’ Counsel

Defendants seek limited discovery of Plaintiffs’ counsel. Def. Mot. Summ. J. 34. They assert that Plaintiffs’ counsel’s knowledge about and use of the disputed emails raises concerns about their ethical conduct and whether they should be permitted to continue to represent Plaintiffs. *Id.* Specifically, Defendants seek to discover the date Plaintiffs’ counsel obtained access to the emails and which emails they reviewed. *Id.* at 35. Since Defendants filed their motion, the Court has resolved this matter. Order, ECF 136. The Court adheres to its prior ruling.

//

//

//

//

//


//

CONCLUSION

Defendants' Motion for Partial Summary Judgment and for Sanctions [106] is DENIED.

IT IS SO ORDERED.

DATED: April 17, 2023.


MARCO A. HERNÁNDEZ
United States District Judge